View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

Journal of Number Theory **96**, 388–399 (2002)
doi:10.1006/jnth.2002.2788

Mordell–Weil Ranks of Quadratic Twists of Pairs of Elliptic Curves

Gwynneth Coogan[1]

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail: gwynneth@math.wisc.edu

and

Jorge Jiménez-Urroz

Departamento de Matemáticas, Facultad de Ciencias, Universidad Autónoma de Madrid, 28049 Madrid, Spain
E-mail: jorge.jimenez@uam.es

Communicated by A. Granville

Received October 11, 2001

Motivated by a conjecture of Mazur, Kuwata and Wang proved that for elliptic curves E^1 and E^2 whose j-invariants are not simultaneously 0 or 1728, there exist infinitely many square-free integers d for which the rank of the Mordell–Weil group of the d-quadratic twists of E^1 and E^2 satisfy: $\mathrm{rk}(E^1_d, \mathbb{Q}) > 0$ and $\mathrm{rk}(E^2_d, \mathbb{Q}) > 0$. Here we present results for the related questions: Are there infinitely many square-free integers d for which: $\mathrm{rk}(E^1_d, \mathbb{Q}) = 0$ and $\mathrm{rk}(E^2_d, \mathbb{Q}) = 0$? And, are there infinitely many square-free integers d for which: $\mathrm{rk}(E^1_d, \mathbb{Q}) = 0$ and $\mathrm{rk}(E^2_d, \mathbb{Q}) > 0$? © 2002 Elsevier Science (USA)

1. INTRODUCTION

Let $E/\mathbb{Q}$ be an elliptic curve defined by

$$E : y^2 = x^3 + ax + b = P(x), \tag{1.1}$$

where $P(x) \in \mathbb{Z}[x]$, and let $L(E, s) = \sum_{n \geqslant 1} \frac{a(n)}{n^s}$ be its associated Hasse–Weil L-function. The coefficients $a(n)$ are completely determined by those with prime index, and if $p \nmid M$ is prime, then

$$a(p) = p + 1 - N(p), \tag{1.2}$$

[1] To whom correspondence should be addressed.

0022-314X/02 $35.00
© 2002 Elsevier Science (USA)
All rights reserved.

where $N(p)$ denotes the number of points in $\tilde{E}$, the reduction of E modulo p, for nonsingular $\tilde{E}$. We now know by the works of Breuil *et al.* [B-C-D-T], Conrad *et al.* [C-D-T], Diamond [D] and Wiles [Wi] that all elliptic curves over $\mathbb{Q}$ are modular, and so $L(E,s)$ is the Mellin transform of a weight 2 newform $F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_2(\Gamma_0(M), \chi_0)$, where M is the geometric conductor of E, χ_0 is the trivial character, and $q = e^{2\pi iz}$.

In this paper we are interested in the family of elliptic curves given by quadratic twists. In particular, for E given by (1.1), we consider the elliptic curve $E_D : Dy^2 = P(x)$ for any fundamental discriminant D. In this case $L(E_D, s)$ is, up to at most finitely many Euler factors, the Hecke L-function of the twisted modular form $(F \otimes \chi_D)(z) = \sum_{n \geqslant 1} \chi_D(n)a(n)q^n$, where $\chi_D(\cdot)$ is the Kronecker character associated with the quadratic field $\mathbb{Q}(\sqrt{D})$.

A well-known conjecture of Goldfeld [G] asserts that

$$\sum_{|D|<X} \mathrm{rk}(E_D, \mathbb{Q}) \sim \frac{1}{2} \sum_{|D|<X} 1,$$

where $\mathrm{rk}(E, \mathbb{Q})$ is the rank of the Mordell–Weil group of E over the rationals. Goldfeld's conjecture together with the Birch and Swinnerton-Dyer conjecture, from now on BSD conjecture, which states that $\mathrm{rk}(E, \mathbb{Q})$ is equal to the order of vanishing of $L(E,s)$ at $s = 1$, implies that the rank of almost every curve E_D is dictated by the sign of the functional equation of $L(E,s)$. Goldfeld's conjecture remains open. In fact, if we consider the quantities $M_E^r(X) = \#\{|D| < X : \ \mathrm{rk}(E_D, \mathbb{Q}) = r\}$, it is not even known that

$$M_E^r(X) \gg X \tag{1.3}$$

for $r = 0, 1$.

While Iwaniec and Sarnak [I-S] prove (1.3) under the Riemann hypothesis, unconditional results are still far from optimal. If we restrict to $r = 0$, the best result in full generality is due to Ono and Skinner [O-S]. They proved $M_E^0(X) \gg X/\log X$. Ono [O] improved the result to $M_E^0(X) \gg X/(\log X)^{1-\alpha}$ for some positive α and any elliptic curve E over $\mathbb{Q}$ without rational 2-torsion. There are, however, cases where this weaker conjecture for $r = 0$ is known to be true including the case of a semistable elliptic curve with rational 3-torsion and good reduction at 3, proved by Vatsal [V2], those of James and Ono [J-O,J], or in the case of certain elliptic curves with full 2-torsion over $\mathbb{Q}$.

For $r = 1$ less is known. The best general result is given by Perelli and Pomykala [P-P] who showed $M_E^1(X) \gg X^{1-\varepsilon}$.

We have to mention the work of Vatsal [V1] where he proved the conjecture for the modular curve $X_0(19)$:

THEOREM A. *Let E be the curve $X_0(19)$. Then we have the estimate*

$$M_E^r(X) \gg X,$$

for $r = 0, 1$.

For two nonisogenous elliptic curves, E^1 and E^2, it is natural to consider whether the following statements are true:

(i) There exist infinitely many square-free integers d such that $\mathrm{rk}(E_d^1, \mathbb{Q}) > 0$ and $\mathrm{rk}(E_d^2, \mathbb{Q}) > 0$.

(ii) There exist infinitely many square-free integers d such that $\mathrm{rk}(E_d^1, \mathbb{Q}) > 0$ and $\mathrm{rk}(E_d^2, \mathbb{Q}) = 0$.

(iii) There exist infinitely many square-free integers d such that $\mathrm{rk}(E_d^1, \mathbb{Q}) = 0$ and $\mathrm{rk}(E_d^2, \mathbb{Q}) = 0$.

These assertions are closely related with Mazur's conjecture about the topological closure of the set of rational points on algebraic varieties $V/\mathbb{Q}$ (see [Ma, Conjectures 1 and 4] for details). In fact Kuwata and Wang, in their work [K-W] on Mazur's conjecture prove assertion (i) for elliptic curves whose j-invariants are not simultaneously 1728 or 0. However, little progress has been made in the direction of (ii) or (iii).

This note concerns assertions (ii) and (iii). In the direction of (ii) we state two results. Using the results given by James [J], concerning elliptic curves related to special ternary quadratic forms, and Vatsal [V1], concerning twists of the modular curve $X_0(19)$, we obtain the following theorem.

THEOREM 1. *Let E be an elliptic curve over $\mathbb{Q}$ which is associated to two ternary quadratic forms in the sense of Theorem C below. Suppose that $3 \nmid d_{Q_1}$ and that $R \neq \emptyset$. Then, for a certain integer $q > 0$ fixed, a positive proportion of positive square-free integers d have the property that*

$$\mathrm{rk}(E_{-3qd}, \mathbb{Q}) = 0 \qquad \textit{and} \qquad \mathrm{rk}(X_0(19)_d, \mathbb{Q}) = 1.$$

Assuming BSD, we can give an affirmative answer to question (ii) for a general elliptic curve.

THEOREM 2. *Let $E^1/\mathbb{Q}$ be an elliptic curve with conductor M_1 and $E^2/\mathbb{Q}$ an elliptic curve with conductor M_2, and let*

$$\mathscr{D}_X := \{d, \text{ a fundamental discriminant } \mid |d| < X\}.$$

Assuming the BSD conjecture, if M_1 and M_2 are coprime, then

$$\#\{d \in \mathscr{D}_X \mid \mathrm{rk}(E_d^1, \mathbb{Q}) = 0 \text{ and } \mathrm{rk}(E_d^2, \mathbb{Q}) > 0\} \gg_{E^1, E^2} X/\log X.$$

In the direction of (iii) we prove

THEOREM 3. *Let* $E^1 : y^2 = P_1(x)$ *and* $E^2 : y^2 = P_2(x)$ *be two elliptic curves over* $\mathbb{Q}$ *without* $\mathbb{Q}$ *rational* 2*-torsion points. Then there exist fundamental discriminants* D_1, D_2 *and a set of primes* T *of positive density such that*

$$\mathrm{rk}(E^1_{dD_1}, \mathbb{Q}) = \mathrm{rk}(E^2_{dD_2}, \mathbb{Q}) = 0,$$

where d *is any product of an even number of distinct primes in* T.

While the BSD conjecture remains open, the study of ranks of elliptic curves is still intimately related to the study of the critical values of L-series. In fact, a celebrated theorem of Kolyvagin [K], allows us to conclude quite a bit about an elliptic curve based on the behavior of its L-series. For our purpose it will be enough to know the following particular case of his theorem,

THEOREM B. *If* E *is an elliptic curve defined over* $\mathbb{Q}$ *with* $\mathrm{ord}_{s=1}(L(E,s)) \leqslant 1$, *then* $\mathrm{rk}(E, \mathbb{Q}) = \mathrm{ord}_{s=1}(L(E,s))$.

There have been many works on the behavior of the central critical values of the L-functions of a general newform with trivial Nebentypus $F(z) = \sum_{n \geqslant 1} a(n)q^n \in S_{2k}(\Gamma_0(N), \chi)$. In the case of families of quadratic twists, a well-known theorem of Waldspurger [W] reveals that the values of the twisted L-functions at the critical point $L(F \otimes \chi_D, k)$ are encoded by the coefficients of certain half integral weight modular forms. Via this theorem, Ono [O] was able to prove a general result about nonvanishing of L-functions for quadratic twists of an even weight newform. His result comes from a combination of Waldspurger's Theorem and his own Theorem 2.2 [O]. However, this device is more general, and a straightforward modification of these arguments allow us to prove the analogous result for two families of twists simultaneously. In particular, we prove:

THEOREM 4. *For* $i = 1, 2$, *let* $F_i(z) = \sum_{n=1}^{\infty} a_i(n)q^n$ *be weight* $2k_i$ *newforms of levels* N_i, *and trivial character*, *and let* K *be a number field containing the coefficients* $a_i(n)$. *Consider a place* v *of* K *over* 2. *If there exists a prime* $p \nmid 2N_1N_2$ *such that*

$$\mathrm{ord}_v(a_1(p)) = \mathrm{ord}_v(a_2(p)) = 0, \tag{1.4}$$

then there exist a set of primes T *of positive density and fundamental discriminants* D_1, D_2 *such that*

$$L(F_{dD_1}, k_1)L(F_{dD_2}, k_2) \neq 0,$$

whenever d is a product of an even number of distinct primes in T not dividing $D_1 D_2$.

In view of Theorem 4, applied to the case of $k_1 = k_2 = 1$, the proof of Theorem 3 is a matter of verifying the technical condition (1.4) for the coefficients of the L-functions of E^1 and E^2. We will use definition (1.2) of the coefficients $a(p)$ and Galois theory for this purpose.

2. PROOF OF THEOREMS 1 AND 2

We begin by stating James' theorem for convenience. To do so we introduce some notation. Let Q be a primitive positive definite ternary quadratic form with discriminant d_Q and denote the square-free part of d_Q by d_Q^{sf}. Then define $\theta_Q = \sum_{x,y,z \in \mathbb{Z}} q^{Q(x,y,z)}$. It is well known that θ_Q is a modular form of weight 3/2, and a theorem of Siegel states that $(\theta_{Q_1} - \theta_{Q_2})$ is a cusp form whenever Q_1 and Q_2 are two primitive positive definite ternary quadratic forms belonging to the same genus. Moreover, given a newform f and a Dirichlet character χ we know that $f \otimes \chi(z)$ is a Hecke eigenform and there exist a newform $f \cdot \chi(z)$ with the same eigenvalues as $f \otimes \chi(z)$ for all but finitely many Hecke operators.

THEOREM C. *Suppose that Q_1 and Q_2 are the only even integral primitive positive definite ternary quadratic forms in a genus of forms. Let A_i denote the number of automorphs of Q_i $(i = 1, 2)$. Assume that $3 \nmid A_1 A_2$ but $3 | A_1 + A_2$. Suppose also that $f = (\theta_{Q_1} - \theta_{Q_2}) \in S_{3/2}(N; \chi_q)$ is a Hecke-eigenform which lifts through the Shimura correspondence to a cusp form $F \in S_2(N/2)$. Let G denote the unique weight 2 newform of trivial character having $\lambda_p(F) = \lambda_p(G)$ for all but finitely many of the primes p and let N_G denote the level of G. Put $R = \{a \in (\mathbb{Z}/4d_{Q_1}^{\mathrm{sf}}\mathbb{Z})^* : \exists$ a square-free $n \equiv a (\mathrm{mod}\, 4d_{Q_1}^{\mathrm{sf}})$ with $3 \nmid a_n(f)\}$, and*

$$\delta = \frac{\#R}{8 d_{Q_1}^{\mathrm{sf}} \prod_{p | d_{Q_1}^{\mathrm{sf}}} (1 - \frac{1}{p^2})}.$$

Then, the set of square-free natural numbers n such that $L(G \cdot \chi_{-qn}, 1) \neq 0$ has lower density at least δ in the square-free natural numbers.

The proof of the above theorem relies on a theorem of Davenport and Heilbronn [D-H] as improved by Nakagawa and Horie [N-H]. In particular let m, T be two positive integers satisfying the conditions:

(i) If p is an odd prime and $p | (m, T)$ then $p^2 | T$, and $p^2 \nmid m$.

(ii) If $2 | T$ then, either $4 | T$ and $m \equiv 1 (\mathrm{mod}\, 4)$ or $16 | T$ and $m \equiv 8$ or $12 (\mathrm{mod}\, 16)$.

Let $T_2^-(m,T)$ be the set of discriminants Δ_d of the imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ for $d<0$ in the arithmetic progression $\Delta_d \equiv m(\mathrm{mod}\, T)$ and denote $h(\Delta_d)$ the class number of the field $\mathbb{Q}(\sqrt{d})$.

THEOREM D. *With the notation above there exist a subset S of $T_2^-(m,T)$ having lower density at least $1/2$ in $T_2^-(m,T)$ such that if $\Delta_d \in S$ then $3 \nmid h(\Delta_d)$.*

Proof of Theorem 1. For the proof we will combine Theorem C with Theorem IV in [V1].

Using the notation of Theorem C, we say that n is a *good* number if for some $a \in (\mathbb{Z}/4\cdot d_{Q_1}^{\mathrm{sf}}\mathbb{Z})^*$ we have

- $n>0, n \equiv 21, 33 \pmod{4\cdot 9}, (n,19)=1$,
- 19 is inert in $\mathbb{Q}(\sqrt{n})$,
- $n \equiv a \pmod{4d_{Q_1}^{\mathrm{sf}}}$.

Let

$$R = \{a \in (\mathbb{Z}/4\cdot d_{Q_1}^{\mathrm{sf}}\mathbb{Z})^* : \exists \text{ square-free } n \text{ good, and } 3 \nmid a_n(f)\}.$$

Suppose that $3 \nmid d_{Q_1}$ and that $R \neq \emptyset$. Then applying Theorem D to $m = a \in R$ and $T = 4\cdot 9\cdot 19 d_{Q_1}^{\mathrm{sf}}$, we see that for a set of positive density of square-free good integers $n \equiv a(\mathrm{mod}\, T), 3 \nmid h(\Delta_{-n})$. Hence, analogously to the proof of Theorem C [J, Proposition 3.1] we deduce that for a set of positive density of square-free good integers $n \equiv a(\mathrm{mod}\, T)$ we have, for G in Theorem C, $L(G\cdot\chi_{-qn}) \neq 0$ and $3 \nmid h(\Delta_{-n})$. In addition, if we write $n = 3c$ and consider, following the notation in [V1] the quadratic fields $k = \mathbb{Q}(\sqrt{c}), k' = \mathbb{Q}(\sqrt{-3c})$ with quadratic Galois characters associated ψ and ψ', respectively, and $\mathscr{F}$ the form parametrizing $X_0(19)$, then c is in the conditions of Theorem IV in [V1] and we conclude by following the argument in that theorem that $s=1$ is a simple zero of $L(\mathscr{F}\otimes\psi, s)$, the L-function of the c-quadratic twist of $X_0(19)$. We just have to use Theorem B to deduce Theorem 1 for the curves E_{-3cq} and $X_0(19)_c$ for a positive proportion of square-free integers c. ∎

An immediate example is obtained by letting E be the curve of conductor 14 that is associated to the modular form obtained from the following two quadratic forms:

$$Q_1(x,y,z) = x^2 + 7y^2 + 7z^2$$

and

$$Q_2(x,y,z) = 2x^2 + 4y^2 + 7z^2 - 2xy.$$

For this curve, by looking at the first 200 coefficients of the modular form, $f = (\theta_{Q_1} - \theta_{Q_2})$, James found that for all congruence classes in $\mathbb{Z}/56\mathbb{Z}$ that are congruent 1,5 or 7 mod 8 and 1, 2 or 4 mod 7, there is a square-free n with $3 \nmid a_n(f)$. Therefore, there are 162 residue classes in $\mathbb{Z}/7 \cdot 8 \cdot 9 \cdot 19\mathbb{Z}$ which meet these congruence requirements and those of [V1]. By Theorem D, at least 1/2 of the square-free integers in these congruence classes have class number not divisible by 3.

Proof of Theorem 2. As in the previous section, let $F(z) \in S_2(\Gamma_0(M), \chi_0)$ be a new form associated to certain elliptic curve E and $F \otimes \chi_D(z)$ be the D-quadratic twist of $F(z)$ for D such that $\gcd(D, M) = 1$.

It is well known (see [I]) that the complete L-function $\Lambda(F \otimes \chi_D, s)$ is entire and verifies the functional equation

$$\Lambda(F \otimes \chi_D, s) = \varepsilon \cdot \chi_D(-M)\Lambda(F \otimes \chi_D, 2 - s),$$

where ε is the sign of the functional equation for $\Lambda(F, s)$.

Notice that if $\varepsilon\chi_D(-M) = -1$ then $L(F \otimes \chi_D, 1)$ is trivially zero. Let $F^1(z), F^2(z)$ be associated to E^1 and E^2 in Theorem 2, respectively. We will look for fundamental discriminants such that $\varepsilon_1\chi_D(-M_1) = -\varepsilon_2\chi_D(-M_2)$. Following the notation in Corollary 3 in [O-S] (see [O-S, Definition]), consider the sets $\pi = \{p \text{ prime} : p \mid M_1M_2\}$ and $\varepsilon \in \{\pm 1\}^{|\pi|}$ such that

$$P(\varepsilon, \pi) = \{d \text{ fundamental discriminant } |\varepsilon_1\chi_D(-M_1) = -\varepsilon_2\chi_D(-M_2)\}.$$

Since $(M_1, M_2) = 1$, a direct application of Corollary 3 of [O-S] to either F^1 or F^2 together with BSD conjecture implies the theorem. ∎

Remark. There are more ways to assure that the signs of the functional equations of two L-series associated to two modular elliptic curves twisted by a common fundamental discriminant are different, but this one will suffice for our purposes here.

3. PROOF OF THEOREMS 3 AND 4

From now on, given any newform $F(z) = \sum_{n \geqslant 0} a(n)q^n \in S_{2k}(N, \chi)$, we will call $g_F(z) = \sum_{n \geqslant 0} b(n)q^n$ the half integral weight modular form guaranteed by a refinement of Waldspurger's theorem by Ono and Skinner. We will use the notation and statement of this result given by Theorem 3.4 in [O]. Then,

$$b^2(D) = C(D)L(F \otimes \chi_D, 1) \tag{3.1}$$

for some $C(D) \neq 0$ and any odd discriminant D. Moreover, if $\lambda(p)$ are the eigenvalues of the Hecke operators $T_k^{\chi}(p^2)$ for $g_F(z)$, then

$$\lambda(p) = \chi^2(p)a(p). \tag{3.2}$$

Consider the classical theta function $\theta(z) = 1 + 2\sum_{n \geqslant 1} q^{n^2}$ and let $G_F(z) = g_F(z)\theta(z) \in S_{k+1}(\Gamma_0(4MN), \tilde{\chi})$.

Let $F_1(z) = \sum_{n \geqslant 0} a_1(n)q^n$ and $F_2(z) = \sum_{n \geqslant 0} a_2(n)q^n$ be as in Theorem 4. The crucial step comes from Theorem 2.2 in [O], where the author shows that for any finite set of integral weight modular forms $\{f_i(z)\}$ of weights k_i there is a set of primes with positive Frobenius density such that the coefficients of $f_i(z)|T_p^{k_i,\chi_i}$ are congruent modulo the prime v as in Theorem 4 for all primes in this set and all of the set of integral weight modular forms. Apply this theorem to the pair $G_{F_1}(z), G_{F_2}(z)$, and the prime p given by (1.4). We find a set of primes T of positive density such that

$$G_{F_i}(z)|T_q^{\tilde{\chi}_i} \equiv G_{F_i}(z)|T_p^{\tilde{\chi}_i} (\mathrm{mod}\ v), \tag{3.3}$$

for $i = 1, 2$ and any $q \in T$. We now recall Lemma 3.3 in [O].

LEMMA E. *Suppose that* $g(z) = \sum_{n=1}^{\infty} b(n)q^n \in S_{k+\frac{1}{2}}(\Gamma_0(4N), \chi)$ *is an eigen form of the Hecke operators* $T_k^{\chi}(p^2)$ *with eigenvalues* $\lambda(p)$ *where* k *is a positive integer. If* $k = 1$, *then make further assumption that the image of* $g(z)$ *under the Shimura correspondence is a cusp form. Let* K *be a number field with the property that all the coefficients* $b(n)$ *and the values of* χ *are in* O_K, *the ring of integers of* K. *Let* v *a place of* K *over* 2. *Define* s_0, n_0 *by*

$$s_0 := \mathrm{ord}_v(b(n_0)) = \min\{\mathrm{ord}_v(b(n))\}$$

and let $g(z)\theta(z) = \sum_{n=1}^{\infty} b_G(n)q^n$. *Then*,

$$\mathrm{ord}_v(b(n)) = s_0 \text{ if and only if } \mathrm{ord}_v(b_G(n)) = s_0. \tag{3.4}$$

Moreover, if there is a prime $p \nmid 4N$ *for which*

$$\mathrm{ord}_v(\lambda(p)) = 0, \tag{3.5}$$

then there exist a set of primes of positive density T *such that for any* d *which is a product of an even number of distinct primes in* T *we have*

$$\mathrm{ord}_v(b(dn_0)) = s_0.$$

Proof of Theorem 4. We apply Lemma E to the eigenforms $g_{F_1}(z) = \sum_{n=1}^{\infty} b_1(n)q^n$, $g_{F_2}(z) = \sum_{n=1}^{\infty} b_2(n)q^n$. Note that (3.5) is satisfied by (3.2) and (1.4). So, by using (3.3) and (3.4), Lemma E gives us a pair of odd integers n_0

and n_0' and a set of primes T of positive density for which $\mathrm{ord}_v(b_1(dn_0)) = \min\{\mathrm{ord}_v(b_1(n))\}$ and $\mathrm{ord}_v(b_2(dn_0')) = \min\{\mathrm{ord}_v(b_2(n))\}$ for any d product of an even number of primes in T. The result now follows by (3.1) ∎

We now turn to the proof of Theorem 3. We will need to satisfy condition (1.4) where $a_1(p)$ and $a_2(p)$ will be given by (1.2) for E^1 and E^2, respectively. In this case, we will prove that $a_i(p)$ for $i = 1, 2$ are odd integers.

By direct computation in (1.2), we see that for primes p of good reduction, the coefficients $a(p)$ of the Hasse–Weil L-function are odd precisely when $P(x)$ is irreducible mod p. Let us call $P(x)_p$ the reduction of $P(x)$ modulo the prime p. Then, proving (1.4) is the same as finding a prime p for which both $P_1(x)_p$, $P_2(x)_p$ are irreducible in $\mathbb{Z}/p\mathbb{Z}$. We now introduce the Galois Theory we will need for this purpose. We will follow the notation in Chapter 4 of Marcus [M].

Consider the tower of extensions $\mathbb{Q} \subseteq K \subseteq L, [L : K] = n, [L : \mathbb{Q}] = ln, L$ normal over K, for number fields K and L. Let R and S be the rings of integers of K and L, respectively. Let $G(L/K)$ denote the Galois group of L over K.

Assume p is a prime in $\mathbb{Z}$ that is unramified in L. Let $\mathfrak{p} \in R$ lie over p and let $\mathfrak{q} \in S$ lie over $\mathfrak{p}$.

In this context the decomposition groups $\mathscr{D} = \mathscr{D}(\mathfrak{q}|\mathfrak{p})$ and $D = D(\mathfrak{q}|p)$ of $\mathfrak{q}$ over the primes $\mathfrak{p}$ and p, are cyclic of orders $\mathfrak{f}$ and f, respectively. Since, p is unramified, we know that $\mathfrak{f}\mathfrak{r} = n$ and $fr = ln$ where $p = \mathfrak{q}_1 \cdots \mathfrak{q}_r$, in R and $\mathfrak{p} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ in S. Further, the groups $\mathscr{D}$ and D have as generators the Frobenius automorphisms $\phi(\mathfrak{q}|\mathfrak{p})$ and $\varphi(\mathfrak{q}|p)$, and they satisfy

$$\mathscr{D} = D \cap G(L/K). \tag{3.6}$$

Finally, let

$$\mathscr{T}_f = \{p \in \mathbb{Z} \text{ prime} : \mathrm{ord}(\varphi) = f\}$$

and

$$T_P = \{p \in \mathbb{Z} \text{ prime} : P(x)_p \text{ is irreducible in } \mathbb{Z}/p\mathbb{Z}\}$$

and for any set of rational primes $T, d(T)$ will be its density over the set of primes.

LEMMA 5. *If $P(x)$ is a cubic irreducible polynomial, then $d(T_P) = 1/3$ or $2/3$.*

Proof. It is well known that the Galois group of the splitting field of a cubic polynomial, $P(x)$, over $\mathbb{Z}$ is S_3 or $\mathbb{Z}_3$. Let α be a root of $P(x)$. Using the

notation given above, let $K = \mathbb{Q}(\alpha), L = L_P =$ splitting field of $P(x)$. Then $l = 3$ and $n = 1$ or 2. It is a basic fact that $P(x)_p$ is irreducible in $\mathbb{Z}/p\mathbb{Z}$ if and only if p is inert in $\mathbb{Q}(\alpha)$. Furthermore, this is equivalent to $f = 3$. Indeed, if $L_P = \mathbb{Q}(\alpha)$ the result is a trivial consequence of $rf = 3$. So we suppose $[L : \mathbb{Q}(\alpha)] = 2$. If p is inert in $\mathbb{Q}(\alpha), r = \mathfrak{r}$ and so $f = 3\mathfrak{f}$. However, since S_3 has no elements of order 6, $f = 3$.

On the other hand, suppose $f = 3$. Then, by (3.6) it is clear that $\mathfrak{f} = 1$, hence $r(\mathfrak{q}|\mathfrak{p}) = 2$ and there cannot be more primes in R over p.

Now, since $G(L/\mathbb{Q}) = S_3$ or $\mathbb{Z}_3$, there are two elements of order 3 and so the Chebotarev density theorem give us $d(T_P) = 1/3$ or $2/3$, respectively. ∎

We now prove the technical condition (1.4). In fact, we prove the following stronger result.

LEMMA 6. *Let $\{P_1(x), P_2(x)\} \in \mathbb{Z}[x]$ be two irreducible cubic polynomials over $\mathbb{Q}$. There exists a set of primes T of positive density such that for any $p \in T, P_1(x)_p, P_2(x)_p$ are irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$ simultaneously.*

Proof. Let α_1, α_2 be roots of $P_1(x), P_2(x)$, respectively and $\mathscr{L}$ the composition field $L_{P_1}L_{P_2}$. Again with the notation given above, let $L = \mathscr{L}$, and $K = \mathbb{Q}(\alpha_1)$. Repeating the argument in Lemma 5 with $\mathscr{L}$ replacing L_P, we find that $f = 3\mathfrak{f}$ for any prime $p \in T_{P_1}$. By considering in the same way $K = \mathbb{Q}(\alpha_2)$, we find that the same is true for any prime $p \in T_{P_2}$. In particular, we have

$$1 - \sum_{3 \nmid f} d(\mathscr{T}_f) \geqslant d(T_{P_1}) + d(T_{P_2}) - d(T_{P_1} \cap T_{P_2}). \tag{3.7}$$

Suppose $[L_{P_1} : \mathbb{Q}(\alpha_1)] = 1$. Then, $\sum_{3 \nmid f} d(\mathscr{T}_f) \geqslant d(\mathscr{T}_1) = 1/[\mathscr{L} : \mathbb{Q}]$ by Chebotarev density theorem. The result now follows from (3.7) and Lemma 5. Hence, we suppose that $[L_{P_1} : \mathbb{Q}(\alpha_1)] = [L_{P_2} : \mathbb{Q}(\alpha_2)] = 2$. By Galois Theory we know that

$$G(L/\mathbb{Q}) \cong G(L/L_{P_1}) \times G(L_{P_1}/\mathbb{Q})$$

and

$$G(L/L_{P_1}) \cong G(L_{P_2}/L_{P_1} \cap L_{P_2}).$$

It is clear that $[L_{P_1} \cap L_{P_2} : \mathbb{Q}] = 1, 2, 3$ or 6. Hence $G(\mathscr{L}/\mathbb{Q}) \cong S_3 \times S_3, S_3 \times \mathbb{Z}_3, S_3 \times \mathbb{Z}_2$ or S_3, respectively.

If $[L_{P_1} \cap L_{P_2} : \mathbb{Q}] \neq 2$, the result is a direct consequence of $\sum_{3|f}(\mathscr{T}_f) < 2/3$, Lemma 5 and (3.7).

If $[L_{P_1} \cap L_{P_2} : \mathbb{Q}] = 2$ we just have to note that $\tilde{\mathfrak{f}} = 1$ or 3 and so $f = 3$ since there are no elements of order 9. The result now follows as in the previous case since $d(\mathscr{T}_3) < 2/3$. ∎

Proof of Theorem 3. Let $L(E^1, s) = \sum_{n \geqslant 1} \frac{a_1(n)}{n^s}, L(E^2, s) = \sum_{n \geqslant 1} \frac{a_2(n)}{n^s}$ be the Hasse–Weil L-functions of E^1 and E^2, respectively. By the modularity of elliptic curves and Lemma 6, there are infinitely many primes p such that

$$a_1(p) \equiv a_2(p) \equiv 1 (\mathrm{mod}\, 2).$$

Hence, the result follows by Theorems 4 and B. ∎

ACKNOWLEDGMENTS

Coogan thanks the National Science Foundation for their generous support. Jiménez-Urroz was partially supported by a fellowship from CAM and FSE. The authors thank Ken Ono for motivating and supporting the research presented herein. We thank the referee for pointing out a mistake in the previous statement of Theorem 1 and for helpful comments and suggestions.

REFERENCES

[B-C-D-T] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), 843–939.

[C-D-T] B. Conrad, F. Diamond, and R. Taylor, Modularity of certain potentially Barsotti–Tate Galois representations, *J. Amer. Math. Soc.* **12** (1999), 521–567.

[D] F. Diamond, On Deformation rings and Hecke rings, *Ann. Math.* **144** (1996), 137–166.

[D-H] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), 405–420.

[G] D. Goldfeld, "Conjectures on Elliptic Curves over Quadratic Fields," Springer Lecture Notes, Vol. 751, Springer, Berlin, pp. 108–118, 1979.

[I] H. Iwaniec, "Topics in Classical Automorphic Forms," Graduate Studies in Mathematics, Vol. 17, Amer. Math. Soc., Providence, RI, 1997.

[I-S] H. Iwaniec and P. Sarnak, The non-vanishing of central values of automorphic L-functions and Landau–Siegel zeros, *Israel J. Math.* **120** (2000), 155–177.

[J] K. James, L-series with non-zero central critical value, *J. Amer. Math. Soc.* **11** (1998), 635–641.

[J-O] K. James and K. Ono, Selmer groups of quadratic twists of elliptic curves, *Math. Ann.* **314** (1999), 1–17.

[K] V.A. Kolyvagin, On the Mordell–Weil group and the Shafarevich–Tate group of modular elliptic curves, *in* "Proceedings of the International Congress of Mathematicians, Kyoto, August 21–29, 1990," Vols. I and II, (Ichirô Satake, Ed.), Mathematical Society of Japan, Tokyo, Springer-Verlag, Tokyo, 1991.

[K-W] M. Kuwata and L. Wang, Topology of rational points on isotrivial elliptic surfaces, *Internat. Math. Res. Notes* **4** (1993), 113–123.

[M] D.A. Marcus, "Number Fields," Springer-Verlag, New York, 1977.

[Ma] B. Mazur, The topology of rational points, *Exp. Math.* **1** (1992), 35–45.

[N-H] J. Nakagawa and K. Horie, Elliptic curves with no torsion points, *Proc. AMS* **104** (1988), 20–25.

[O] K. Ono, Nonvanishing of quadratic twists of modular *L*-functions and applications to elliptic curves, *J. Reine Angew. Math.* **533** (2001), 81–97.

[O-S] K. Ono and C. Skinner, Non-vanishing of quadratic twists of modular *L*-functions, *Invent. Math.* **34.3** (1998), 651–660.

[P-P] A. Perelli and J. Pomykala, Averages of twisted elliptic *L*-functions, *Acta Arith.* **80**, No. 2 (1997), 149–163.

[T-W] R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke algebras, *Ann. Math.* **141** (1995), 553–572.

[V1] V. Vatsal, Rank-one twists of a certain elliptic curve, *Math. Ann.* **311** (1998), 791–794.

[V2] V. Vatsal, Canonical periods and congruence formulae, *Duke Math. J.* **98.2** (1999), 397–419.

[W] J.L. Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier, *J. Math. Pures Appl.* **60** (1981), 375–484.

[Wi] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. Math.* **141** (1995), 443–551.